UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/656,751 | 09/04/2003 | Matthew A. Stillerman | 1032-005US01 | 9058 |

28863 7590 09/07/2007
SHUMAKER & SIEFFERT, P. A.
1625 RADIO DRIVE
SUITE 300
WOODBURY, MN 55125

| EXAMINER | |
|---|---|
| NALVEN, ANDREW L | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/07/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/656,751 | STILLERMAN ET AL. | |
| | Examiner | Art Unit | |
| | Andrew L. Nalven | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *24 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) *9-17,26-34,42-46 and 55-64* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,18-25,35-41 and 47-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-54 are pending.

### *Election/Restrictions*

**2.** Claims 9-17, 26-34, 42-46, and 55-64 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 6 March 2007.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1-5, 7, 18-22, 24, 47-51, and 53 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Drews US Patent No. 6,463,535 in view of Kozen "Efficient Code Certification."

4. **With regards to claims 1, 18, and 47**, Drews teaches that upon power-up of a computer, retrieving boot code and a certificate from a peripheral device coupled to the

computer (Drews, column 3 lines 7-25, downloads boot image and signed manifest over communication link), verifying with the computer, security of a boot code associated with a peripheral device by performing a security check on the boot code in accordance with a certificate (Drews, column 5 lines 32-60, signed manifest is accessible by the verification function, manifest is verified) and executing the boot code based on a result of the security check (Drews, column 5 lines 30-40, application image can be executed if verification function returns success). Drews fails to teach a description of the operation of the boot code being verified. However, Kozen teaches a description of the operation of the boot code being verified (Kozen, pages 2-3, structured annotations that direct the verification process, verifier checks set of conditions that are sufficient to imply desired safety properties). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kozen's method of verifying operation of a program because it offers the advantage of allowing ensuring that executable code downloaded from an untrusted source is safe to run (Kozen, page 2).

5. **With regards to claims 2, 19, and 48**, Crews as modified teaches verifying the security of the boot code includes verifying the boot code via Efficient Code Certification that specifies a process for performing the security check on the boot code as indicated by the certificate (Kozen, pages 2-3).

6. **With regards to claims 3, 20, and 49,** Drews as modified teaches the certificate further indicates a type of security check to perform (Kozen, pages 2-3, directs verification process).

7. **With regards to claims 4, 21, and 50**, Drews as modified teaches the type of security check comprises one of a security check to enforce type safety, a security check to enforce flow control safety, a security check to enforce memory safety, a security check to enforce stack safety, a security check to enforce device encapsulation, and a security check to enforce prevention of specific forms of harm (Kozen, page 3, control flow, memory, stack safety).

8. **With regards to claims 5, 22, and 51**, Drews as modified teaches the boot code includes boot firmware (Drews, column 3 lines 7-25, boot image).

9. **With regards to claims 7, 24, and 53**, Drews as modified teaches verifying the safety of the boot code occurs inline such that verifying the safety of the boot code occurs in real time prior to executing the boot code (Drews, column 3 lines 7-25, pre-boot operation state).

10. **Claims 2, 23, and 52 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Drews US Patent No. 6,463,535 and Kozen "Efficient Code Certification," as applied to claim 1 above, and in further view of Rudoff et al US Patent No. 6,263,378

11. **With regards to claims 2, 23, and 52**, Drews as modified fails to teach the boot firmware conforms to the Open Firmware standard IEEE-1275. However, Rudoff teaches boot firmware conforming to the Open Firmware standard IEEE-1275 (Rudoff, Abstract). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Rudoff's method of using IEEE 1275 because it offers

the advantage of providing facilities for both debugging hardware and software and provides an industry standard (Rudoff, column 3 lines 10-30).

12. **Claims 35-41 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Drews US Patent No. 6,463,535 in view of Kozen "Efficient Code Certification" and Ong US PGPub 2004/0177258.

13. **With regards to claim 35**, Drews as modified teaches all that is described above regarding claim 1, but fails to teach a peripheral device having a memory module wherein the memory module stores a boot code and a certificate. However, Ong teaches a peripheral device having a memory module wherein the memory module stores a boot code and a certificate (Ong, paragraph 0025). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ong's method of storing boot codes and certificates in a peripheral device because it offers the advantage of allowing the identification and verification of a peripheral component using its certificate to prove trust (Ong, paragraph 0028).

14. **With regards to claims 36**, Drews as modified teaches verifying the security of the boot code includes verifying the boot code via Efficient Code Certification that specifies a process for performing the security check on the boot code as indicated by the certificate (Kozen, pages 2-3).

15. **With regards to claims 37,** Drews as modified teaches the certificate further indicates a type of security check to perform (England, column 7 lines 18-46, component certificate, Kozen, pages 2-3).

16. **With regards to claims 38**, Drews as modified teaches the type of security check comprises one of a security check to enforce type safety, a security check to enforce flow control safety, a security check to enforce memory safety, a security check to enforce stack safety, a security check to enforce device encapsulation, and a security check to enforce prevention of specific forms of harm (Kozen, page 3, control flow, memory, stack safety).

17. **With regards to claims 39**, Drews as modified teaches verifying the safety of the boot code occurs inline such that verifying the safety of the boot code occurs in real time prior to executing the boot code (Drews, column 3 lines 7-25, pre-boot operation state).

18. **With regards to claim 41**, England as modified teaches the peripheral device comprises one of a graphic device, network controller, and storage controller (Ong, paragraph 0025, stores sensitive data).

19. **Claims 8, 25, and 54 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Drews US Patent No. 6,463,535 and Kozen "Efficient Code Certification," as applied to claims 1, 18,and 47 above, and in further view of England US Patent No. 6,757,824,

20. **With regards to claims 8, 25, and 54**, Drews as modified fails to teach the boot code includes a device driver to initialize a peripheral device and define an application program interface for accessing and controlling the peripheral device. However, England teaches the boot code includes a device driver to initialize a peripheral device

and define an application program interface for accessing and controlling the peripheral device (England, column 7 lines 35-47). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize England's method of initializing a device driver because it offers the advantage of ensuring that all components of the operating system are trusted and helps ensure that all storage will be secure (England, column 1 lines 50-65).

21. **Claim 40 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Drews US Patent No. 6,463,535 in view of Kozen "Efficient Code Certification" and Ong US PGPub 2004/0177258, as applied to claim 35, and in further view of England US Patent No. 6,757,824.

**With regards to claims 40**, Drews as modified fails to teach the boot code includes a device driver to initialize a peripheral device and define an application program interface for accessing and controlling the peripheral device. However, England teaches teach the boot code includes a device driver to initialize a peripheral device and define an application program interface for accessing and controlling the peripheral device (England, column 7 lines 35-47). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize England's method of initializing a device driver because it offers the advantage of ensuring that all components of the operating system are trusted and helps ensure that all storage will be secure (England, column 1 lines 50-65).

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER